(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 August 2001 (09.08.2001)

PCT

(10) International Publication Number
WO 01/57807 A1

(51) International Patent Classification[7]: G07C 9/00, G07F 7/10

(21) International Application Number: PCT/US00/14191

(22) International Filing Date: 23 May 2000 (23.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/498,902 4 February 2000 (04.02.2000) US

(71) Applicant: 3M INNOVATIVE PROPERTIES COMPANY [US/US]; 3M Center, P.O. Box 33427, Saint Paul, MN 55133-3427 (US).

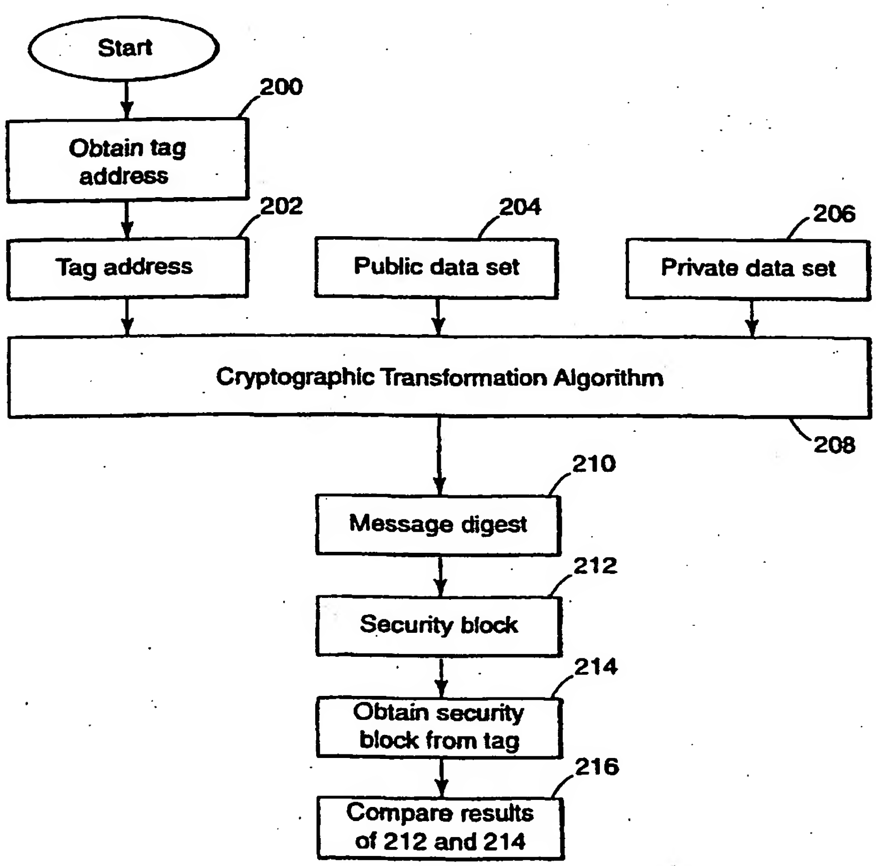
(72) Inventors: BALDWIN, Robert, W.; P.O. Box 33427, Saint Paul, MN 55133-3427 (US). PIOTROWSKI, Chester; P.O. 33427, Saint Paul, MN 55133-3427 (US). SEVCIK, Paul, A.; P.O. 33427, Saint Paul, MN 55133-3427 (US).

(74) Agents: OLSON, Peter, L. et al.; Office of Intellectual Property Counsel, P.O. Box 33427, Saint Paul, MN 55133-3427 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: METHOD OF AUTHENTICATING A TAG



(57) Abstract: A method is disclosed for authenticating, for example, radio frequency identification (RFID) tags by providing an RFID tag having a stored security block that is cryptographically related to the tag address, obtaining the tag address from the tag, cryptographically transforming at least the tag address and a private data set to obtain a security block, and then comparing that security block to the stored security block. If the two security blocks match, then the tag can be presumed to be authentic. Alternatively, the stored security block can be cryptographically transformed using at least a private data set to obtain a tag address, and that tag address can then be compared with the stored tag address. If the two tag addresses match, then the tag can be presumed to be authentic.

WO 01/57807 A1

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD OF AUTHENTICATING A TAG

Field of the Invention

The invention relates to a method of authenticating a device, tag, label, or similar item, and in one embodiment to a method of cryptographically verifying a tag of a matched component system so that hardware that is part of the matched component system will only interrogate tags that are authenticated as part of the matched component system.

Background of the Invention

Encryption has been used for many years to make information secure against the efforts of those who should not have access to that information. Information is first encoded by a first authorized user, and then decoded by a second authorized user to obtain access to the information. An example of simple encryption would be to equate a unique number with each letter of the alphabet, and then to represent the information of interest using those numbers, instead of letters. A person who knows the encryption algorithm (the substitution of a unique number for each letter) could then decode the information to obtain access to it. This type of simple encryption is easily broken however, and thus is not very secure.

Other more sophisticated forms of encryption have been used, particularly in modern times, to secure information that is to be electronically transferred from one authorized user to another. For example, it is often desirable to transmit private information such as a message, credit card number, or the like over the Internet, and thus to encrypt that information in a suitably secure manner. A suitable type of encryption for these purposes is the "public/private key" encryption technique that is described in common texts and patents on encryption.

The patent literature includes a number of references related to the uses of encryption for tracking manufactured articles, or for performing article authentication. See, for example, European Patent Application 0 710 934 A2, entitled "Methods and Systems for Performing Article Authentication"; European Patent Application 0 889 448 A2, entitled "Method of Preventing Counterfeiting of Articles of Manufacture"; and U.S. Patent No. 5,768,384, entitled "System for Identifying, Authenticating and

Tracking Manufactured Articles." The methods described in these and other references are not, however, suitable for use with tags as a means of authentication, as described below with reference to the present invention.

Summary of the Invention

Tags or labels containing information about an article can be provided as part of a matched component system along with the hardware used to read, scan, or interrogate those tags or labels. Examples of such systems include bar code labels (or printing equipment) and scanners, and radio frequency identification (RFID) tags and RFID interrogators. One reason to encourage the use of matched component systems is to enable the system to avoid interrogating tags belonging to another system. Thus, error messages may be reduced, and it may be possible to use two or more systems to identify various materials in the same location. Another reason is related to the product or system warranties. That is, manufacturers often warrant their products for a given period or to perform a given function only if they are used with other components with which they have been repeatedly tested by the manufacturer, but offer no warranty or a reduced warranty if they are not. In the case of a matched component system of the type described herein, a system provider may warrant the operation of the system if a tag interrogator is used in conjunction with authentic tags, but not otherwise. Specifically, a system provider may warrant the operation of an RFID system when that provider sells the RFID tags, and also sells the equipment used to write information to, and/or read information from, those tags.

The authentication method described herein enables a system or user to authenticate, for example, radio frequency identification (RFID) tags by providing an RFID tag having a stored security block that is cryptographically related to the tag address, obtaining the tag address from the tag, applying a cryptographic transformation to at least the tag address and a private data set to obtain a security block, and then comparing that security block to the stored security block. If the two security blocks match, then the tag can be presumed to be authentic. Alternatively, the stored security block can be cryptographically transformed using at least a private data set to obtain a tag address, and that tag address can then be compared with the stored tag address. If the two tag addresses match, then the tag can be presumed to be

authentic. Also described is an RFID tag for use with the present invention. The invention finds particularly useful application in the interrogation by portable or stationary RFID interrogators of RFID tags placed in library materials, such as books.

Brief Description of the Drawings

The present invention is described in greater detail with reference to the appended Figures, in which:

Figure 1 is a process diagram illustrating one embodiment of the inventive method for providing a tag with a security block that is a cryptographic transformation of the tag address;

Figure 2 is a process diagram illustrating one embodiment of the inventive method for authenticating a tag by field encryption and comparison;

Figure 3 is a process diagram illustrating one embodiment of the inventive method for authenticating a tag by field decryption and comparison; and

Figure 4 is a schematic diagram of an RFID tag in accordance with the present invention.

Detailed Description of the Invention

I. Overview

In simple terms, a preferred method of authenticating an RFID tag according to the present invention involves the following steps. First, a tag address that identifies the tag is obtained from the memory of the tag. Second, the tag address and a private data set, and optionally a public data set, are cryptographically transformed to provide a security block that is stored in the memory of the tag. Third, when it is desired to authenticate the tag, the tag address is again obtained and, along with the data set(s) is cryptographically transformed to provide a security block that is compared with the stored security block. Or, alternatively, the security block is cryptographically transformed, using the inverse of the original transformation, including appropriate data set(s), to obtain a tag address that is compared to the stored tag address. Fourth, if the two security blocks (or tag addresses, depending on which process was used) are the same, then the tag is authentic. If not, the tag is not authentic.

These steps, and other features, variations, and embodiments of the present invention are described in greater detail below. Although the invention is described in terms of an RFID system, other systems in which information can be read from and written to a tag (preferably electronically) are also within the scope of the present invention.

II. The Tag

An RFID tag suitable for use in conjunction with the present invention is described in PCT Publication 99/65006 entitled "Identification Tag With Enhanced Security," the rights to which are assigned to the assignee of the present invention. As shown in Figure 4, RFID tag 10 generally includes an antenna 12 connected to a memory device 14 such as an integrated circuit (IC). The tag may include a power source, such as a battery or capacitor, or may be powered solely by the RFID interrogator such that it receives both energy and information in the form of radio waves from the RFID interrogator. The tag may be provided with adhesive (typically pressure sensitive adhesive) so that it may be adhered to, for example, a library book. It will be appreciated by those skilled in the art that Figure 4 represents only one of the many embodiments of geometry and antenna design suitable for use in an RFID tag.

A commercial example of a suitable RFID tag is one available from the Texas Instruments Company of Dallas, Texas, under the designation "TIRIS Tag-it." The Tag-it brand RFID tag includes a first memory storage area that stores unalterable data (referred to as "permanent tag memory"), such as unique unalterable data identifying that specific tag (referred to herein as the "tag address"), and a second memory storage area that stores variable information provided by a user (referred to herein as "variable tag memory"). Current Tag-it brand RFID tags include 256 bits of variable tag memory, although more memory is likely to become available on that and other RFID tags in the future. The Tag-it brand RFID tag operates at a 13.56 MHz communication frequency, although tags and interrogators that operate at other frequencies may be used instead. Tag-it brand RFID tag systems may also be used with Windows-compatible software available from Texas Instruments to simplify the use of Tag-it brand RFID tags and equipment.

A. Permanent Tag Memory

It is preferred that the tag address is stored in the permanent tag memory. It is also preferred that this tag address be unique to insure that it is possible to identify and address a specific tag during use. This tag address might, for example, be 32 bits long, allowing over 4 billion unique addresses. Typically this tag address is programmed into the tag during manufacture and "factory locked" so that it cannot be changed later. A tag address may include information stored in both the permanent tag memory and the variable tag memory, described below.

B. Variable Tag Memory

Variable tag memory, subject to any applicable restrictions on the amount of memory available, may be used to store information about the manufacturer of the tag or the tag itself (such as when and where the tag was made), and/or about the article to which the tag is attached or to be attached. For example, where the RFID tag will be attached to a library book or other material, the title, author, call number, checkout status, and usage statistics associated with that book may be stored in the variable tag memory. Other information that may be stored in the variable tag memory includes the name of the library that owns the book or material, the specific library branch from which it was borrowed, the appropriate location (such as the specific shelf location) for the book or material, type of item (book, CD, video tape), and the like.

A portion of the variable tag memory may be locked, so that it cannot be inadvertently modified. For example, the data on a tag associated with an item belonging to a library can thereby be protected from accidental modification by an RFID-based airline baggage handling system or other RFID writer. The locking procedure differs among RFID tag suppliers. In the case of the Texas Instruments Tag-it brand RFID tags, the smallest block of variable memory that can be locked in this manner is 32 bits, which may be used to store certain cryptographically transformed information in the manner described herein.

III. Readers (Interrogation Sources) and Writers (Programmers)

RFID tags used in one embodiment of the invention are both readable and programmable. That is, the RFID tag can be read or interrogated by an interrogation

source to obtain some or all of the information stored in the variable tag memory of the tag for use or manipulation by a user, and can also be programmed (written) with information provided by a system or user. Suitable RFID interrogation sources and RFID writers are commercially available from Texas Instruments of Dallas, Texas under the designation "Commander 320."

In one embodiment of the present invention, certain information is cryptographically transformed and written into a portion of the available variable tag memory by an RFID writer, and in use the tag is interrogated by an RFID reader that determines whether the tag is authentic, as described in greater detail below. RFID readers preferably can interrogate multiple RFID tags virtually simultaneously (the Commander 320 brand interrogation source currently is able to interrogate 30 RFID tags per second), though this feature is not required.

<u>IV. Encryption</u>

Before the tag can be authenticated, certain information is obtained from the tag and other information is stored on it. Specifically, the tag address is obtained from the tag, cryptographically transformed as described below, and the resulting security block is then stored on the tag. One exemplary process for providing a tag having a stored security block in accordance with the present invention is shown in Figure 1.

Step 100 is to read or interrogate the tag to obtain the tag address 102. The tag address is then concatenated with at least one data set, and preferably two data sets. If one data set is used, then that data set should be a private data set 106 that is not generally available to the public, but is stored in and used by the interrogation source. If two data sets are used, as exemplified in the remainder of this description, then one data set may be private and the other a public data set 104, as represented in Figure 1. The tag address and the data set(s) could be interleaved or otherwise scrambled (instead of being concatenated) if desired, though this is not believed to add significantly to the security or reliability of the system.

The public and private data sets may consist of any string of characters and/or numbers, and can be human readable strings that are represented as binary data using

standard methods such as ASCII, UTF-8 or Unicode. The public data set may be widely distributed or not, as desired. In other words, the public and private data sets are simply two data sets, which may have different levels of secrecy imposed on them by the user. The data set(s), and particularly the private data set, is preferably a string of random characters and/or numbers, so that it is difficult or impossible to reverse engineer the data set from the cryptographically transformed information. To create the data set(s), a random or substantially random process may be used, such as a random number generator.

The public or private data set may be subsumed within software used to create and authenticate the tags. The software, in general, will consist of machine language instructions, which are not readily intelligible to people and cannot be deciphered except by highly specialized individuals expending a great deal of time. Thus, the data set(s) will preferably be sufficiently difficult to locate within that software that it may be considered for all practical purposes to be private even when the software itself is widely distributed. The form of the public or private data sets may also be chosen to facilitate legal protection under copyright, trade secret or other law, so that any unauthorized user of the data set(s) would also be infringing on a legally protected right.

Although the tag address, the public data set, and the private data set may be of any desired length and content, by way of example the tag address may have, for example, 32 bits of information, the public data set may have at least 32 bytes of information, and the private data set may have at least 32 bytes of information. An exemplary tag address could be the hexadecimal value 0x012345678, and exemplary public data set may be the ASCII string "3M Radio Frequency Identification Systems," and an exemplary private data set may be 0x0001E2882AC7B5C613FAF447170E90702957A5053C5C013D7235168E268DE990.

The tag address 102 and private data set 106, and optionally the public data set 104, are then fed into a cryptographic transformation algorithm 108, such as a cryptographic hash algorithm, which transforms the data and outputs a message digest

110 of, for example, 160 bits in length. Cryptographic transformations encompass both conventional reversible encryption such as the Data Encryption Standard (DES, which is also referred to as the Data Encryption Algorithm (DEA) by ANSI, and as the DEA-1 by the ISO), and other related techniques such as the use of a one-way cryptographic hash such as the Secure Hash Algorithm 1, or SHA1. Examples of both types of algorithms along with detailed source code in the C programming language are including in the book Applied Cryptography, Protocols, Algorithms, and Source Code in C, by Bruce Schneier (John Wiley and Sons, Inc. 1996 (2d edition)) beginning at page 442, and in the Handbook of Applied Cryptography, A. Menezes et al. (CRC Press 1997) beginning at page 348. Although other cryptographic algorithms such as DES-CBC-MAC and DES-DMAC may be used as the cryptographic transformation method of the present invention, cryptographic hash algorithms such as SHA1, MD5, and RIPEMD-160 are preferred because they provide a relatively high level of security against attempts to reverse-engineer the private data set when the message digest and the public data set are known, and also because they are readily available, easy to implement, and free of significant governmental restrictions on use. The source code associated with the SHA1 described in the Applied Cryptography reference cited above is currently available on computer disc from Bruce Schneier, Counterpane Systems, 7115 W. North Ave., Suite 16, Oak Park, IL 60302-1002.

If, due to variable tag memory limitations, it is desirable not to store the entire message digest on the tag, then a specified portion of the message digest may be designated and stored in (written to) the variable tag memory of the RFID tag. This portion of the message digest is security block 112. Additionally, if it is desired to lock the security block in the variable tag memory against inadvertent alteration, as described above, then a lockable unit or block of the variable tag memory, perhaps 32 bits, may determine the appropriate size of the security block of information from among the message digest which should be designated and stored in the variable tag memory. It may also or instead be desirable to store the message digest or the security block in the permanent tag memory, which would normally be done by or for the manufacturer of the tag. For convenience, the output of the cryptographic transformation (such as SHA1) will be referred to as the "message digest," and the entirety or portion of the message digest that is stored on the RFID tag will be referred

to as the "security block." Thus the security block 112 may be created by designating at least part of the message digest, and then written to the RFID tag in the manner described above as shown at 114.

V. Authentication

Once a security block that represents the message digest, or a portion of the message digest, from a cryptographic transformation has been stored on a tag, the tag may be used for authentication in the field. Authentication may be performed in several different manners, two of which are described below. The first involves following the same process used to encrypt the tag, and then comparing the result (the security block) with the stored security block to determine whether they are the same. If the two security blocks are the same, then the tag is authentic. If they are different, then the tag is not authentic. This is referred to as "field encryption and comparison."

The second authentication process described below involves essentially the reverse. That is, the authentication process begins by obtaining the stored security block from the memory of the tag, performing an encryption transformation in reverse using the private data set and, if needed, the public data set, to obtain a tag address. The tag address is then compared with the stored tag address. If the two tag addresses are the same, then the tag is authentic. If they are different, then the tag is not authentic. This is referred to as "field decryption and comparison." In order to use this second authentication process, the security block should comprise the entire message digest.

These authentication processes are described in further detail with reference to Figures 2 and 3.

A. Field Encryption and Comparison

Figure 2 illustrates the field encryption and comparison process steps used to determine whether a certain tag is authentic. The user in the field follows the same method as shown in Figure 1, and then compares the resulting value with the stored security block to determine whether the tag is authentic.

In the embodiment shown in Figure 2, steps 200 through 212 are the same as their counterparts in Figure 1. That is, the tag address is obtained 200; the tag address 202, the private data set 206, and optionally the public data set 204 are provided to the cryptographic transformation algorithm 208 that provides a message digest 210, from which a security block is created 212. To authenticate the tag by comparison, the RFID reader obtains the stored security block from the tag, as shown at 214, and compares the results (shown as 216) of the security block 212 with the stored security block obtained from the tag at 214. If the two security blocks are the same, then the tag is authentic. If the two messages do not match, then the user could conclude that the item is not authentic, and take any appropriate action. Such action could, for example, include terminating processing of the item to which the tag was affixed.

<u>B. Field Decryption and Comparison</u>

Figure 3 illustrates the field decryption and comparison process steps used to determine whether a certain tag is authentic. As shown in Figure 3, the security block (which in this embodiment should be identical to the message digest) is obtained from the tag 300; the security block 302, the private data set 306, and optionally the public data set 304 are provided to the cryptographic transformation algorithm 308 that provides the tag address 310. The RFID reader then obtains the stored tag address from the tag 312, and compares the results (shown as 314) of the tag address 310 with the stored tag address at 312. If the two tag addresses are the same, then the tag is authentic. If the two tag addresses are not the same, the tag is not authentic. The cryptographic transformation can be a reversible block cipher, stream cipher, or other suitable process.

The cryptographic transformation 308 could be the inverse of the cryptographic transformation used to create the security block stored on the RFID tag. In one embodiment, the cryptographic transformation could be a block cipher such as DES running in encrypt mode (to encrypt the security block) and decrypt mode (to field decrypt the security block), where the key to the block cipher would be a function of the public and private data sets. For example, the data set(s) could be passed through a cryptographic hash function to produce a 160-bit message digest and a predetermined subset of these bits would be selected to create the 56-bit key for the DES block cipher.

For block ciphers like RC5 that accept long keys, the key could be a concatenation or other predetermined arrangement of the bits that make up the data set(s).

VI. Variations of the Inventive Process

It will be appreciated that certain steps shown in Figures 1, 2, and 3 can be done in an order different than that shown in the respective illustrations. For example, in Figure 2 the step 214 of obtaining the stored security block from the tag could take place at an earlier stage in the process, perhaps even as the first step in the process. Similarly, in Figure 3 the step 312 of obtaining the stored tag address from the tag could take place at an earlier stage in the process. Also, although the tag address, the public data set, and the private data set are shown as independent inputs into the cryptographic transformation algorithm, they can as described above be concatenated, interleaved, or otherwise grouped prior to being input to the cryptographic transformation algorithm.

In other embodiments the role of the tag address and security block can be reversed. This reversal can be useful when the tag address and security block are stored such that one is more difficult to change than the other. If the tag manufacturer writes the tag address and the application vendor writes the security block, then reversing the roles of the tag address and security block may be useful in some circumstances.

The present invention is described in even greater detail in regard to the following Example.

EXAMPLE

This Example is a representation of an arbitrary tag address, public data set, and private data set that could be used in conjunction with the method of the present invention. A tag address, expressed in hexadecimal, could be 0x12345678. This address would be concatenated with an ASCII-string public data set "Copyright (c) 2000, 3M IPC. All Rights Reserved", which in hexadecimal notation is "0x43 0x6f 0x70 0x79 0x72 0x69 0x67 0x68 0x74 0x20 0x28 0x63 0x29 0x20 0x32 0x30 0x30 0x30 0x2c 0x20 0x33 0x4d 0x20 0x49 0x50 0x43 0x2e 0x20 0x41 0x6c 0x6c 0x20 0x52 0x69 0x67 0x68 0x74 0x73 0x20 0x52 0x65 0x73 0x65 0x72 0x76 0x65 0x64".

This concatenated data would further be concatenated with a hexadecimal private data set "0xe0 0x34 0xc7 0xf0 0xf9 0xf7 0x37 0x26 0xf6 0x19 0x53 0x15 0x11 0x64 0xe5 0x30 0x45 0x4b 0xe3 0xbf 0x6a 0xca 0xdc 0x6e 0xbe 0xb4 0x84 0xe3 0xb1 0x2d 0x77 0x38", which could be generated by computer using a pseudo-random number generator. The full concatenated string would be processed using the SHA1 cryptographic hash algorithm, and the resulting message digest, expressed in hexadecimal, would be 0x3385275891ceb2e69cdc4a56031276413d6d702d. From that one could select the low-order nibble (4 bits) of each of the first eight (8) bytes of the message digest (shown as the underlined characters in the preceding message digest) which would then be concatenated to provide a security block, expressed in hexadecimal, of 0x35781e26 that could be stored on an RFID tag by an RFID writer. The tag could then be authenticated by using the field encryption and comparison process described above to determine whether the tag was authentic.

The authentication method described herein finds particularly useful application in the authentication of RFID tags used with library materials such as books. A portable (handheld, for example) RFID interrogator may be used to interrogate the RFID tags and, if the tags are authentic, to obtain other information from the RFID tag that is useful to library staff members. Stationary RFID interrogators such as patron self-service devices, staff work stations, and stations at which library materials having only optical bar codes are converted to have RFID tags, may also use the authentication method of the present invention.

Although most of the foregoing disclosure has been in the specific context of the authentication of RFID tags by an RFID reader through the use of certain encryption (and in some cases decryption) techniques, variations of the methods described are also within the scope of the invention. For example, tags, readers, and writers that operate at frequencies other than radio frequencies may be used in place of those described. With suitable modifications, the present invention may be adapted for use with bar codes (including two-dimensional bar codes), wherein a bar code address would be substituted for an RFID tag address, and the like.

We claim:

1. A method of providing an RFID tag with a security block, comprising the steps of:

(a) obtaining the tag address;

(b) performing a cryptographic transformation on at least the tag address and a private data set to provide a security block; and

(c) storing the security block on the tag.

2. The method of claim 1, wherein the tag includes a permanent tag memory and a variable tag memory.

3. The method of claim 2, wherein the tag address is stored in the permanent tag memory.

4. The method of claim 2, wherein at least part of the tag address is stored in the variable tag memory.

5. The method of claim 2, wherein step (c) comprises storing the security block in the variable tag memory.

6. The method of claim 5, further comprising the step of:

(d) locking at least the portion of the variable tag memory in which the security block is stored to prevent inadvertent modification of the security block.

7. The method of claim 2, wherein step (c) comprises storing the security block in the permanent tag memory.

8. The method of any one of claims 1 through 7, wherein the cryptographic transformation includes the use of a cryptographic hash algorithm.

9. The method of any one of claims 1 through 7, wherein the cryptographic transformation includes the use of a block or stream cipher.

10. The method of any one of claims 1 through 7, wherein step (b) comprises cryptographically transforming at least the tag address and the private data set to provide a message digest, and designating at least a portion of the message digest as the security block.

11. The method of claim 10, wherein the cryptographic transformation includes the use of a cryptographic hash algorithm.

12. The method of any one of claims 1 through 7, wherein step (b) comprises cryptographically transforming the tag address, the private data set, and a public data set.

13. The method of claim 12, wherein step (b) comprises cryptographically transforming the tag address, the private data set, and a public data set to provide a message digest, and designating at least a portion of the message digest as the security block.

14. The method of claim 11, wherein step (b) further comprises cryptographically transforming the tag address, the private data set, and a public data set.

15. The method of claim 12, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

16. The method of claim 13, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

17. The method of claim 14, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

18. The method of claim 12, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

19. The method of claim 13, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

20. The method of claim 14, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

21. A method of authenticating an RFID tag having a stored tag address that identifies the tag and a stored security block derived at least in part from that tag address, comprising the steps of:

(a) obtaining the tag address;

(b) performing a cryptographic transformation on at least the tag address and a private data set to provide a security block; and

(c) comparing the security block of step (b) with the security block stored on the tag to determine whether the two security blocks are the same.

22. The method of claim 21, wherein the tag includes a permanent tag memory and a variable tag memory.

23. The method of claim 22, wherein the tag address is stored in the permanent tag memory.

24. The method of claim 22, wherein at least part of the tag address is stored in the variable tag memory.

25. The method of claim 22, wherein the stored security block is stored in the variable tag memory.

26. The method of claim 25, wherein at least the portion of the variable tag memory in which the stored security block is stored is locked to prevent inadvertent modification of the stored security block.

27. The method of claim 22, wherein the stored security block is stored in the permanent tag memory.

28. The method of any one of claims 21 through 27, wherein the cryptographic transformation includes the use of a cryptographic hash algorithm.

29. The method of any one of claims 21 through 27, wherein the cryptographic transformation includes the use of a block or stream cipher, where the cipher is run in encryption mode.

30. The method of any one of claims 21 through 27, wherein step (b) comprises cryptographically transforming at least the tag address and the private data set to provide a message digest, and designating at least a portion of the message digest as the security block.

31. The method of claim 30, wherein the cryptographic transformation includes the use of a cryptographic hash algorithm.

32. The method of any one of claims 21 through 27, wherein step (b) comprises cryptographically transforming the tag address, the private data set, and a public data set.

33. The method of claim 32, wherein step (b) comprises transforming the tag address, the private data set, and a public data set to provide a message digest, and selecting at least a portion of the message digest as the security block.

34. The method of claim 31, wherein step (b) further comprises cryptographically transforming the tag address, the private data set, and a public data set.

35. The method of claim 32, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

36. The method of claim 33, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

37. The method of claim 34, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

38. The method of claim 32, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

39. The method of claim 33, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

40. The method of claim 34, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

41. A method of authenticating an RFID tag having a stored tag address that identifies the tag and a stored security block derived at least in part from that tag address, comprising the steps of:

(a) obtaining the security block;

(b) performing a cryptographic transformation on the security block using at least a private data set to provide a tag address; and

(c) comparing the tag address of step (b) with the stored tag address to determine whether the two tag addresses are the same.

42. The method of claim 41, wherein the tag includes a permanent tag memory and a variable tag memory.

43. The method of claim 42, wherein the stored tag address is stored in the permanent tag memory.

44. The method of claim 42, wherein at least part of the stored tag address is stored in the variable tag memory.

45. The method of claim 42, wherein the stored security block is stored in the variable tag memory.

46. The method of claim 45, wherein at least the portion of the variable tag memory in which the stored security block is stored is locked to prevent inadvertent modification of the security block.

47. The method of claim 42, wherein the stored security block is stored in the permanent tag memory.

48. The method of any one of claims 41 through 47, wherein the cryptographic transformation includes the use of a block or stream cipher, where the cipher is run in decryption mode.

49. The method of any one of claims 41 through 47, wherein step (b) comprises cryptographically transforming the security block, the private data set, and a public data set to provide the tag address.

50. The method of claim 49, wherein the cryptographic transformation includes the use of a block or stream cipher, where the cipher is run in decryption mode.

51. The method of claim 49, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

52. The method of claim 50, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

53. The method of claim 49, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

54. The method of claim 50, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

55. A method of providing an RFID tag having a stored tag address that identifies the tag and a stored security block derived at least in part from that tag address, and of authenticating the tag, comprising the steps of:

(a) providing the stored security block by

(i) obtaining the tag address;

(ii) performing a cryptographic transformation on at least the tag address and a private data set to provide a security block; and

(iii) storing the security block on the tag; and

(b) authenticating the tag by

(i) obtaining the tag address;

(ii) performing a cryptographic transformation on at least the tag address and the private data set to provide a security block; and

(iii) comparing the security block of step (b)(ii) with the stored security block to determine whether the two security blocks are the same.

56. The method of claim 55, wherein the tag includes a permanent tag memory and a variable tag memory.

57. The method of claim 56, wherein the tag address is stored in the permanent tag memory.

58. The method of claim 56, wherein at least part of the tag address is stored in the variable tag memory.

59. The method of claim 56, wherein step (a)(iii) comprises storing the security block in the variable tag memory.

60. The method of claim 59, wherein at least the portion of the variable tag memory in which the stored security block is stored is locked to prevent inadvertent modification of the stored security block.

61. The method of claim 56, wherein step (a)(iii) comprises storing the security block in the permanent tag memory.

62. The method of any one of claims 56 through 61, wherein the cryptographic transformations in steps (a) and (b) both include the use of a cryptographic hash algorithm.

63. The method of any one of claims 56 through 61, wherein the cryptographic transformations in steps (a) and (b) both include the use of a block or stream cipher.

64. The method of claim 63, wherein the cipher is run in encryption mode.

65. The method of any one of claims 56 through 61, wherein steps (a)(ii) and (b)(ii) comprise cryptographically transforming at least the tag address and the private data set to provide a message digest, and designating at least a portion of the message digest as the security block.

66. The method of claim 65, wherein the cryptographic transformations in steps (a) and (b) include the use of a cryptographic hash algorithm.

67. The method of any one of claims 56 through 61, wherein steps (a)(ii) and (b)(ii) comprise cryptographically transforming the tag address, the private data set, and a public data set.

68. The method of claim 67, wherein steps (a)(ii) and (b)(ii) comprise cryptographically transforming the tag address, the private data set, and a public data set to provide a message digest, and designating at least a portion of the message digest as the security block.

69. The method of claim 66, wherein steps (a) and (b) further comprise cryptographically transforming the tag address, the private data set, and a public data set.

70. The method of claim 67, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

71. The method of claim 68, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

72. The method of claim 69, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

73. The method of claim 67, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

74. The method of claim 68, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

75. The method of claim 69, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

76. A method of providing an RFID tag having a stored tag address that identifies the tag with a stored security block, where the security block is derived at least in part from that stored tag address, and of authenticating the tag, comprising the steps of:

(a) providing the stored security block by
  - (i) obtaining the tag address;
  - (ii) performing a cryptographic transformation on at least the tag address and a private data set to provide a security block; and
  - (iii) storing the security block on the tag; and

(b) authenticating the tag by

(i) obtaining the stored security block;

(ii) performing a cryptographic transformation on at least the stored security block and the private data set to obtain a tag address; and

(iii) comparing the tag address of step (b)(ii) with the stored tag address to determine whether the two tag addresses are the same.

77. The method of claim 76, wherein the tag includes a permanent tag memory and a variable tag memory.

78. The method of claim 77, wherein the tag address is stored in the permanent tag memory.

79. The method of claim 77, wherein at least part of the tag address is stored in the variable tag memory.

80. The method of claim 77, wherein step (a)(iii) comprises storing the security block in the variable tag memory.

81. The method of claim 80, further comprising the step of:

(a) (iv) locking at least the portion of the variable tag memory in which the security block is stored to prevent inadvertent modification of the security block.

82. The method of claim 77, wherein step (a)(iii) comprises storing the security block in the permanent tag memory.

83. The method of any one of claims 76 through 82, wherein the cryptographic transformation includes the use of a block or stream cipher that, in step (a)(ii), is run in encryption mode and, in step (b)(ii), is run in decryption mode.

84. The method of any one of claims 76 through 82, wherein step (a)(ii) comprises cryptographically transforming the tag address, the private data set, and a public data set, and step (b)(ii) comprises cryptographically transforming the security block, the private data set, and the public data set.

85. The method of claim 84, wherein the public data set is "Copyright (c) 2000, 3M IPC. All Rights Reserved".

86. The method of claim 84, wherein the public data set is protectable by copyright, trade secret, trademark, or service mark law.

87. The method of claim 1, wherein the tag address is obtained by an RFID interrogation source, and the security block is stored on the tag by an RFID writer.

88. The method of either of claims 21 or 41, wherein the method is performed by a handheld RFID reader.

89. The method of either of claims 21 and 41, wherein the method is performed by a library patron self-service unit.

90. The method of either of claims 55 and 76, wherein at least step (b) is performed by a portable RFID reader.

91. The method of either of claims 55 and 76, wherein at least step (b) is performed by a stationary RFID reader.

92. An RFID tag, wherein the tag has a stored tag address and a stored security block that is cryptographically related to the tag address.

93. The RFID tag of claim 92, wherein the tag address and a private data set are cryptographically transformed to provide the security block.

94. The RFID tag of claim 92, wherein the tag address, a private data set, and a public data set are cryptographically transformed to provide the security block.

95. The RFID tag of claim 92, wherein the tag includes a permanent tag memory and a variable tag memory.

96. The RFID tag of claim 95, wherein the tag address is stored in the permanent tag memory.

97. The RFID tag of claim 95, wherein at least part of the tag address is stored in the variable tag memory.

98. The RFID tag of claim 95, wherein the security block is stored in the variable tag memory.

99. The RFID tag of claim 95, wherein at least the portion of the variable tag memory in which the stored security block is stored is locked to prevent inadvertent modification of the stored security block.

100. The RFID tag of claim 95, wherein the security block is stored in the permanent tag memory.

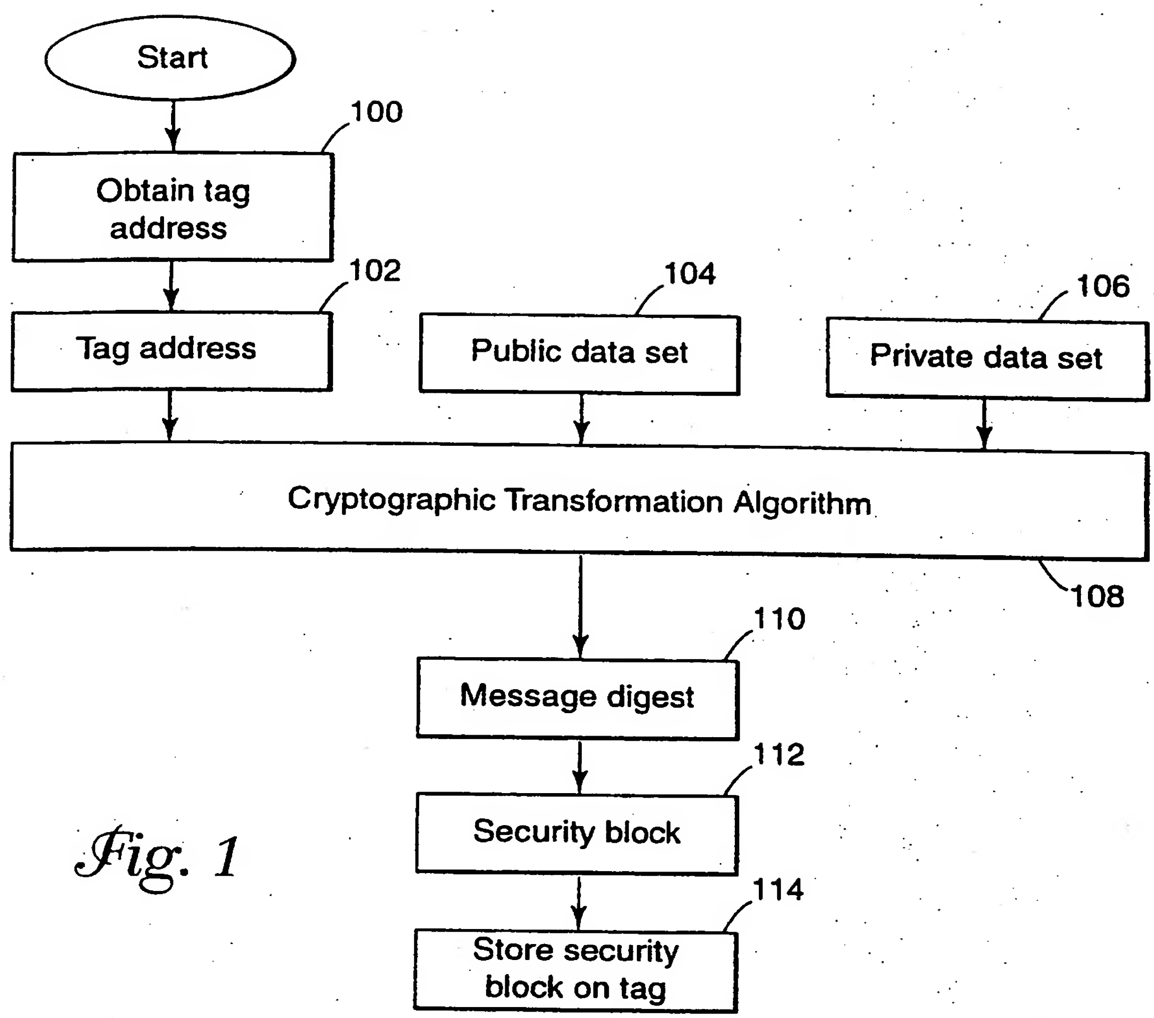

Start
100
Obtain tag address
102
Tag address
104
Public data set
106
Private data set
Cryptographic Transformation Algorithm
108
110
Message digest
112
Security block
114
Store security block on tag

Fig. 1

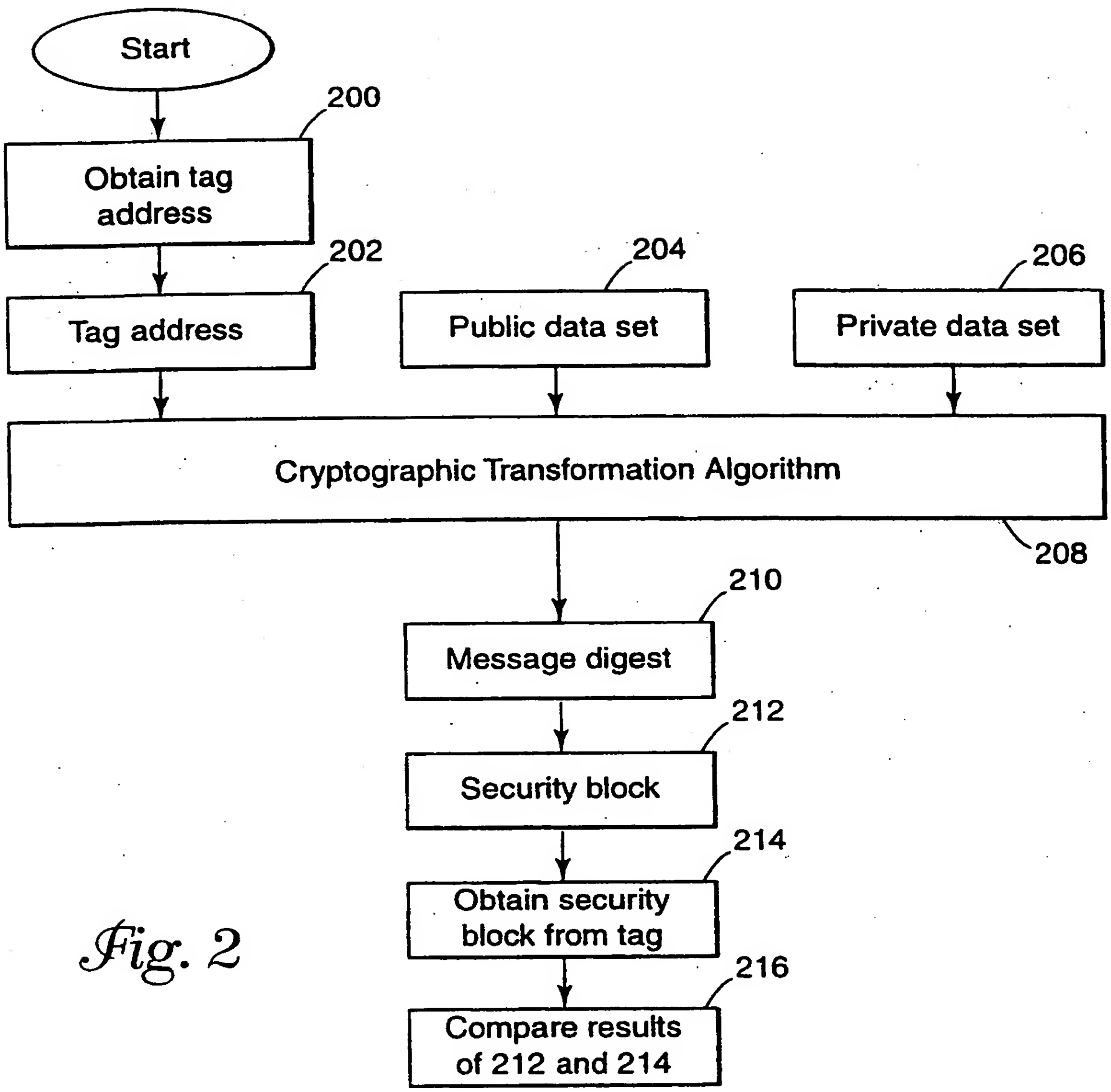

Start
200
Obtain tag address
202
Tag address
204
Public data set
206
Private data set
Cryptographic Transformation Algorithm
208
210
Message digest
212
Security block
214
Obtain security block from tag
216
Compare results of 212 and 214

Fig. 2

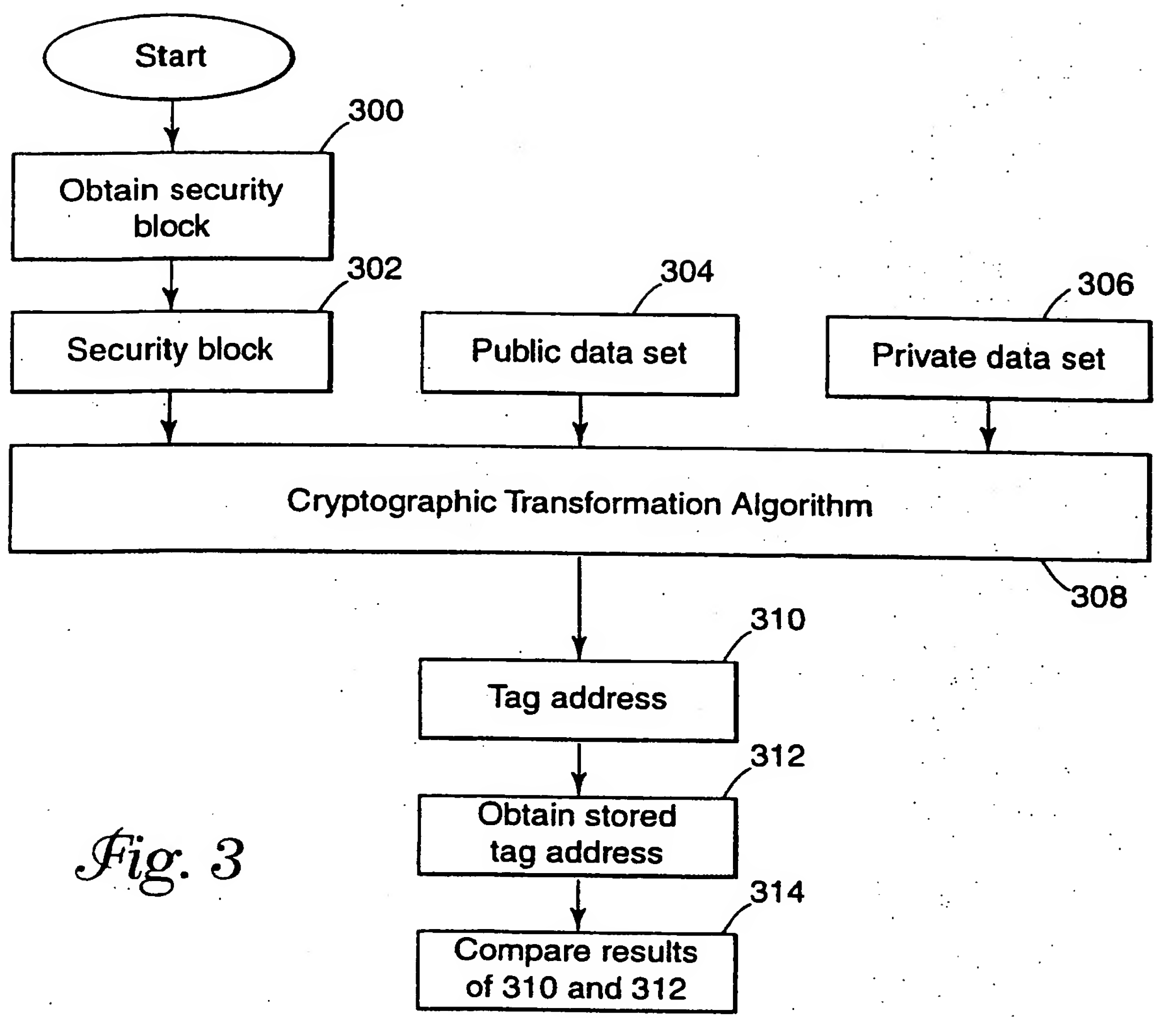

Start
300
Obtain security block
302
Security block
304
Public data set
306
Private data set
Cryptographic Transformation Algorithm
308
310
Tag address
312
Obtain stored tag address
314
Compare results of 310 and 312

Fig. 3

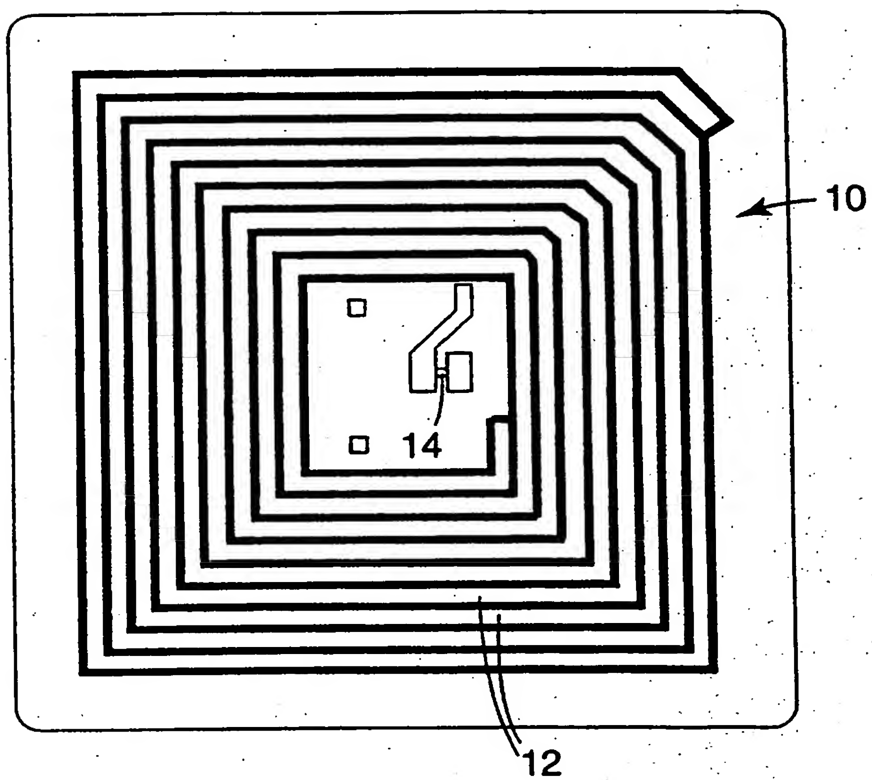


Fig. 4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/14191

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G07F G06K G07D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 758 777 A (PALOMAR TECHN CORP) 19 February 1997 (1997-02-19) column 1, line 3 -column 1, line 6 column 4, line 32 -column 7, line 34	1-3,5,8, 10-14, 87,92-98
Y		6,55-57, 63,67, 69,99
X	FR 2 697 929 A (INNOVATRON SA) 13 May 1994 (1994-05-13) page 11, line 24 -page 17, line 1	21-23, 25,29,32
Y		26
Y	US 5 191 193 A (LE ROUX JEAN-YVES) 2 March 1993 (1993-03-02) column 1, line 10 -column 1, line 22 column 3, line 22 -column 5, line 18	55-57, 63,67,69

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 November 2000	30. 11. 00

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Aupiais, B

1

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/14191

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 764 977 A (STELLA) 24 December 1998 (1998-12-24) page 1, line 1 -page 1, line 24 page 5, line 26 -page 6, line 19 ---	6,26,99
A	EP 0 030 381 A (GREY LAB ESTABLISHMENT) 17 June 1981 (1981-06-17) page 6, line 17 -page 12, line 25 ---	41
A	WO 99 65006 A (MINNESOTA MINING & MFG) 16 December 1999 (1999-12-16) cited in the application page 2, line 2 -page 2, line 17 page 6, line 31 -page 7, line 10 ---	1,21,41, 55,76,92
X,P	EP 0 982 688 A (DATAMARS SA) 1 March 2000 (2000-03-01) the whole document -----	1,8,92

1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 00/14191

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 15-20, 35-40, 51-53, 70-75, 85-86
because they relate to subject matter not required to be searched by this Authority, namely:

The additional features of these claims relate either to presentation of information or method of doing business (Rule 39.1(v) PCT and Rule 39.1(iii) PCT).

2. [ ] Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/14191

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 0758777	A	19-02-1997	US	5832090	A	03-11-1998
			CA	2182464	A	11-02-1997
FR 2697929	A	13-05-1994	NONE			
US 5191193	A	02-03-1993	FR	2653248	A	19-04-1991
			CA	2027344	A,C	14-04-1991
			DE	69014817	D	19-01-1995
			DE	69014817	T	22-06-1995
			EP	0423035	A	17-04-1991
			ES	2066169	T	01-03-1995
			JP	1884135	C	10-11-1994
			JP	3241463	A	28-10-1991
			JP	6009051	B	02-02-1994
			KR	147360	B	01-12-1998
FR 2764977	A	24-12-1998	CN	1260872	T	19-07-2000
			EP	0988511	A	29-03-2000
			WO	9858238	A	23-12-1998
EP 0030381	A	17-06-1981	DE	2949351	A	11-06-1981
			AT	13781	T	15-06-1985
			DE	3070759	D	18-07-1985
			JP	57074772	A	11-05-1982
WO 9965006	A	16-12-1999	AU	1378399	A	30-12-1999
EP 0982688	A	01-03-2000	EP	0982687	A	01-03-2000